International Journal of Applied Operational Research
Vol. 6, No. 4, pp. 53-64, Autumn 2016

Journal homepage: ijorlu.liau.ac.ir

Securing AODV Routing Protocol Against the Black Hole Attack Using Firefly Algorithm

M. Ebrahimi*, S. Jamali

Received: 20 March 2016 **;** **Accepted:** 21 August 2016

Abstract Mobile ad hoc networks are networks composed of wireless devices to create a network with the ability for self-organization. These networks are designed as a new generation of computer networks to satisfy some specific requirements and with features different from wired networks. These networks have no fixed communication infrastructure and for communication with other nodes the intermediate nodes are used. Despite having many benefits due to wireless channel and dependency of each node to the intermediate node, these networks are faced with many security concerns. One of the concerns is the possibility of black hole attacks occurrence. The occurrence of black hole attacks has challenged the security issue in this kind of networks. This type of attack which is applied on mobile ad hoc network routing protocols, declares its black hole node as the shortest route to the destination node and therefore, other nodes in the network select this node as the intermediate node in sending their packets to various destinations. As a result, these nodes can delete received packets instead of sending them to destination. To avoid this problem in mobile ad hoc networks and based on AODV routing protocol, we introduce a new method to immediately identify the black hole attack and prevent it from occurring. To detect and defend against black hole attacks in mobile ad hoc networks, we use Firefly algorithms. Firefly algorithm is a biologically motivated algorithm for multi-faceted optimizing applications which is recently developed and used in many applications. To demonstrate the effectiveness of FireFlyAODV method, we used NS-2 Simulator and compared our work with AODV protocol under black hole attack. The results of simulation show that the proposed method has higher performance in terms of packet delivery ratio, throughput, the number of removed packets and end-to-end delay.

Keywords: Mobile Ad Hoc Networks, Routing, Black Hole Attacks, Firefly Algorithm.

1 Introduction

Mobile ad hoc networks are networks without infrastructure that have been formed by a set of mobile hosts and are connected to each other through wireless links. In these networks, each node can act as a final system and also, can send the packets in the role of a router. In wireless ad hoc networks, two nodes can be connected to each other through one or several steps. Wireless ad hoc networks topology may be alternate and thus the displacement of nodes will be changed; so with this technology nodes can easily change their position. Tools used in

* **Corresponding Author. (✉)**
E-mail: mrt.ebrahimi@gmail.com (M.Ebrahimi)

M. Ebrahimi
Department of Computer Engineering, Germi branch, Islamic Azad University

S. Jamali
Department of Computer Engineering, University of Mohaghegh Ardabili

wireless ad hoc networks can exist in many forms but they have the same basic activity; this means that all the nodes at least have equally autonomy. Routing and security topics in mobile ad hoc wireless networks is one of the most important challenges and among the topics related to security, the topic of attacks on mobile ad hoc networks is always considered. Attack black hole is one of the most important of these attacks where the attacker attracts the network traffic by releasing false routing news for the shortest path and then removes all the sent packets. Black holes attack can take place by one or several nodes. Therefore search and quickly create a path from the source to the destination node for wireless ad hoc networks are crucial. The routing structure in wireless mobile ad hoc networks, which somehow is based on a kind of trust between nodes, provides a good opportunity for attackers so by participating in routing somehow cause disturbance in routing process and eventually disrupt the routing process. One of the famous protocols that are in mobile ad hoc wireless networks is AODV protocol which most of the research have investigated this protocol and the impact of black hole attacks. A black hole attack tries to scramble for routing in addition to eavesdrop and remove the packets and possible threats for the above mentioned features. A black hole attack which are common in wireless ad hoc networks, can take place by one or several nodes. Single node black hole attack forges the numbers chain and the hops number of a routing message that has accessed the path by force, and then eavesdrops all the data packets and begins to remove the packets. Black Hole attacks in mobile ad hoc networks can be seen in many different forms: packet dropping, structure change in routing, diversion in network topology and finally creating fake nodes are examples of these forms, the rest of the paper is organized as follows. An overview of the related works is presented in section 2. A review of black hole attacks is investigated in section 3, AODV routing protocol in mobile ad hoc networks is in section 4, section 5 deals with the proposed method, section 6 provides the results of simulations of the proposed method and finally, section 7 presents the conclusion.

2 Related Work

In the previous section we examined and showed the characteristics of mobile ad hoc networks and also described mobile ad hoc network applications and advantages. In the following, we suggest methods that researchers have suggested to defend against black hole attacks and evaluate some of the proposed works.

Myddyan et al., in 2011 applied the method that uses the number of rules to ensure the honesty of sender's answer. Activities of a node are recorded by its neighbors. These neighbors ask other nodes to send their opinion about this node. When a node gathered the opinions of all its neighbors, it decides if the responder is a destructive node. The decision is based on the number of rules. Judgment is based on the nodes activity in the network. The first rule says that if a node delivers some of data packets to the destination, it is assumed that the node is honest. According to the second rule, if a node receives a number of packets but does not send the same data, the current node may be an abusive or destructive node. When the second rule is correct about a node and if the current node sends some RREP packets, so certainly the current node is abusive or destructive. When the second rule is correct about a node, if the current node is not sending RREP packets, the current node fails. In another work, Patel et al., [3] presented MAV-AODV protocol in 2013 which goal is to increase the multi-part structure survival, maximum packet delivery ratio and overhead management. MAV-AODV is a tree-based protocol, this protocol works based on ACO strategy. When traverse a route, ants leave a trace called Pheromone so among the created routes, other ants choose the

shortest route to food. This protocol has been presented in VANET network where machines periodically send beacon message to one another for selecting the optimal route for their movement. The protocol should check the link survival and as a result, periodically send beacon message. Of the advantages of this protocol are multi-part tree maintenance at the highest level and building stable routes [3]. Tamilarasan et al., [4] presented a method to whether there is more difference between sequence numbers of the source nodes or intermediate node in returning RREP backward or not, and typically, the first response of path (response request table) is higher than the destructive node with sequence number. Now we can compare the first sequence number of destination with the source sequence number. If there is much greater difference in source and destination sequence numbers, thus the destination node is destructive, and we can remove it directly from the response request table. The main advantage of the proposed method is that destructive node is identified at an early stage and we will remove it immediately and the destructive nodes are easily identified without any delay. In another method Karloff and Wagner [5], firstly proposed selective forwarding and then multipath forwarding attacks, which can be used for counting the attacks in sensor networks. However, the algorithm cannot show a way to discover and eliminate attacker from the network[5]. In 2012, Saetang et al., [6] using improved protocol suggested a solution for the single black hole that in this method, next hop information should be attached to RREP packet when each intermediate node responds to the RREQ, then the source node (FREQ) sends a reapply to the next hop of responsive node and the node responsive is detected only if the next hop is reliable. In another work, Yu et al., [7] proposed a method to discover and eliminate holes gray nodes, and all nodes involved in forwarding that should establish stability for receiving data packets. When the source node has some suspicious behaviors, it applies the search algorithm for approval of intermediate nodes and according to search algorithm it detects the destructive by abuse node detection algorithm.

3 Black Hole Attacks in Mobile Ad Hoc Networks

In mobile ad hoc wireless networks there are many attacks, for example, the attacks that disrupt normal process of the network. In this section, we describe black hole attacks and the effect of this kind of attacks on routing protocols [8].

In black hole attack, the attacker attracts network traffic to itself by releasing the routing false news for shortest path. This destructive node sends fake messages to send the shortest path. As a result, the source node ignores checking the routing table and sends the sent packets through this node. Then the black hole node begins to remove sent packets, and this attack causes the service outage. The way how destructive node can fit into the paths is shown in Figure 1. Destructive node 4 listens when the legal node S requests a route to another node that is D; node No. 4 has this information and claims to have the shortest route to get to D. As a result, S will send its packet to 4 and expects the packet to reach to D, but node No. 4 does not send the packet for S. Its consequences can include having nodes with no connection to the rest of the network.

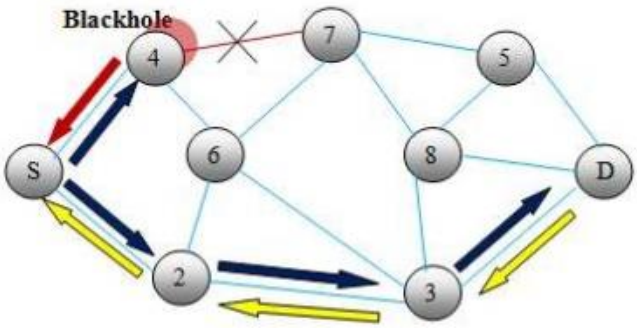

Fig. 1 Examples of black hole attack in mobile ad hoc networks

After drawing the packets of a node to itself, the attacker node selectively throws some of them away and sends the rest.

4 AODV Routing Protocol

This protocol can be considered as an improvement on DSDV protocol. AODV minimizes the number of releases by making route when necessary. In contrast to DSDV that kept a list of all the routes, to find a route to the destination, the source releases a route request packet. Neighbors release the packet for their neighbors. When a source node tries to send a message to several destination nodes and there is no acceptable route to the destination, to find another node, it creates a route discovery process and releases a route request packet RREQ to its neighbors as long as the destination or an intermediate node or a free route to the destination is found. AODV applies ordinal numbers of destination to ensure that all routes have ring freedom and include most recent route information. Each node keeps its ordinal numbers as broadcast identifier. Broadcast identifier increases for each RREQ of node along with IP address so that it is determined for each RREQ of node. Along with ordinal number of identifier broadcast, the source node has the recent ordinal number to the destination in its RREQ. Intermediate nodes can respond to the RREQ only if they have a route to the destination so that the ordinal number of destination is available, greater or equal to the RREQ content. During the process of sending RREQ the intermediate nodes' path records in tables the neighbor address that the first copy of broadcast packet has reached to it, so to make a reverse path. If later the additional copies have reached from the same RREQ these packets are rejected. Once RREQ reached to the destination or intermediate node with a free enough route, the destination node / intermediate node sends a route response packet (RREP) backward using unicast to the neighbor that the first RREQ has reached from it. When RREP is routing along with reverse route, nodes associated with this route put their after route inputs in their route tables which this refers to the node that RREP come of it. These next route inputs specify the next active route. Associated with each route input there is a route timer so that if the input is not used in a specified lifetime, it will be removed because RREP inputs will be sent along with accessed route by RREQ and AODV only supports the use of symmetrical links. Figure 2 and 3 show an example of route discovery in this protocol.

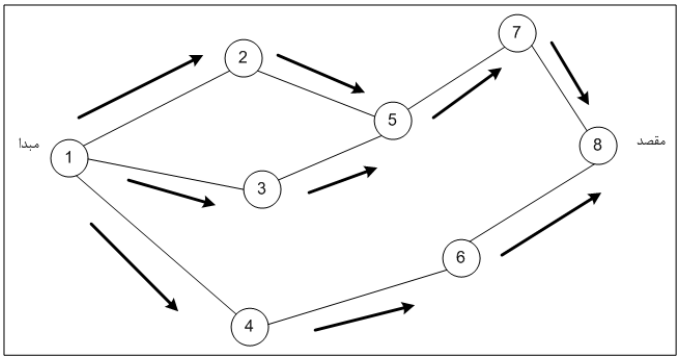

Fig. 2 broadcast for route discovery in AODV

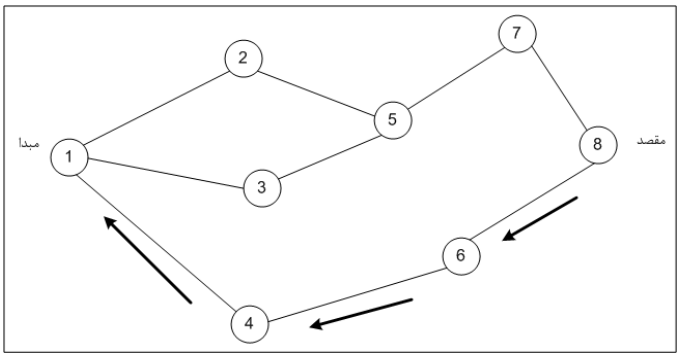

Fig. 3 route discovery in AODV

In Figure 2, when a node sends route request packet for a neighbor, it registers the node from which the first request has come in its table. AODV only uses symmetrical and two-way links, because routing the response packet is done by reversing the packet route, that is, the response packet reaches the source by traversing the same path in reverse order. In Figure 3, nodes which are along this route, enter the route is their table. If the source node moves, the source should re-do the route discovery process to the destination but if one of the intermediate nodes move, then the neighboring node moves and realizes the link failure and sends a link failure notification to neighbors in the opposite direction until it reaches the source node and source can re-do the route discovery if required.

5 The Proposed Method (FireFly AODV)

Among the technologies based on environmental factors, in this paper we use firefly algorithm to detect black hole attack. Firefly algorithm is a biologically motivated algorithm for optimized multi-faceted applications that have been recently developed. Experimental results show that Firefly algorithm is usually more efficient than the Particle Swarm Optimization (PSO) algorithm and Genetic Algorithm (GA).

5.1 Details of the Proposed Method of FireFlyAODV

In this method, we use a timer to collect responses. The received responses are stored in a table called response table. In this method, the truth table is used to verify the reliability of responding nodes in order to detect collective black holes attacks. In this table, a number is assigned to each node as the truth level. For example, the number 2 can be used; by receiving

ack from the destination, the true level of responding node increases and with not receiving ack the true level of responding node and the next hop is reduced by one by source and the new true table will be broadcast. Thus, in the first attack by the black hole it can be said that it loses the chance of another attack and in the worst case, with the second attack its true level of will reach the zero and then will be deleted from routing.

We have explained that in AODV protocol under the black hole attack, the path that has the shortest step and that is the black hole node is selected. In our proposed method based on the firefly algorithm, among the RREPs that arrive to the destination, we choose the ones that in addition to step and distance factors, has the highest attractiveness based on the Firefly algorithm. To do this, we act as follows:

As we mentioned, in the proposed method the shortest route topic has also been considered. So that in response packet, there is geographical location and distance fields and these fields and levels of truth table are used to calculate the attractiveness of responses.

The routing table of each of the nodes should also be changed so that a field called attractiveness should be added in each entry which is superior in terms of the attractiveness from the previous route.

5.1.1 Necessary parameters to assess the attractiveness of received responses

To assess the attractiveness of received responses, the firefly algorithm is used which is shown in Figure 4.

First, the necessary parameters for algorithm are provided:

- The maximum number of fireflies: is calculated after completing the timer duration.
- The objective function for each response i at location x f(x)
- Production of initial population of fireflies which are the same reached responses.

To calculate the objective function the received response fields and the true level of responding node and the next hop has been used and thus we determine the attractiveness of each response. Of course, this calculation only takes place for responses for which total true levels of responding node and the next hop are higher than a threshold and presumed to be reliable. Total true levels of intermediate node and its next hop are calculated using the formula 1. Which, as mentioned, β_0 is absorption in r = 0 and γ is the light absorption coefficient [7]

$$L_i = \beta_0 e^{-\gamma r^2}$$

For many implementation scenarios, we can consider $\beta_0 = 1$ and $\gamma = 1$.

```
While (t <MaxGeneration)
For i = 1: m all m fireflies
For j = 1: i all n fireflies
Light intensity I_i at x_i is determined by f(x_i)
If (Ij > Ii)
Move firefly i top of response table
End if
```

Fig. 4 pseudo-code added to the response table

After sorting the response table by the highest attractiveness, RREP is sent in the most attractive route which is now at the top of the table and after completing the timer ack, true

levels table will be updated by the source and broadcasted. When the true level of a node reaches to zero, a warning message will be broadcasted about it and deleted from routing. So by doing this and choosing this route, the selected route will be free from black hole attacks.

6 Simulation and Evaluation of The Proposed Method

In this section, we evaluate the proposed method of FireFlyAODV using the NS-2 simulator. To demonstrate the effectiveness of our method, we use measures of the number of lost packets, packet delivery ratio, end-to-end delay and throughput.

6.1 Simulation Parameters

For needed simulations in order to evaluate the proposed approach (FireFlyAODV) it has tried to use several scenarios such as those in performed simulations; a summary of the performed simulation parameters can be seen in Table 1.

Table 1 Simulation parameters

Type of simulation	NS2 2.34
700*700	Environment
20	The number of nodes
(AODV)	Routing Protocol
250 meters	Transmission range
Omenia Antenna	Type of antenna
100,200,300,400,500,600	Simulation times
802_11	MAC layer
CBR (UDP)	Type of traffic
150 packets	Buffer Size
Random	Position of nodes
4	The number of black hole nodes

6.2 Evaluation Criteria

End-to-end delay: in mobile ad hoc networks the period in which the information packets are transmitted across the network from source to destination nodes is called end-to-end delay.
Packets delivery ratio: packets delivery rate in mobile ad hoc networks is of the utmost importance. In these networks usually sending the package is done step by step or through several jumps. In this type of network packet delivery ratio is calculated from the formula 2.

$$PDR = \frac{\sum The\ number\ of\ received\ packets\ in\ destination}{\sum The\ number\ of\ sent\ packets}$$

In relation 2, PDR is packet delivery ratio which is achieved by dividing the Number of Received Packet to the Number of Sent Packet.

The number of lost packets: lost packets in mobile ad hoc networks can happen for various reasons, for example, sent packets failed to reach the destination node in the network, or packets be lost based on bit error or faulty hardware. Noise existence in the network can also be caused by packet loss. Another factor of the loss of packets in mobile ad hoc networks is the loss of node energy during sending the packet. This parameter is calculated with the formula 3.

Lost Packet=(Sent Packet-Received Packet)/Sent Packet

Throughput: throughput is considered as the essential and key criteria in mobile ad hoc networks. Hence for evaluating the proposed method, we also examined this criterion. Figure 4-5 shows that the proposed method of FIREFLYAODV has a better performance compared to AODV protocol under black hole attack at different times. The reason for this is that the proposed approach makes more number of packets reach their destination per time unit, therefore, FIREFLYAODV method at the same time unit has higher throughput compared to AODV protocol under attack.

6.3 Simulation Results

We carried out the simulations on the proposed approach and made sure that FireFlyAODV works properly. The simulation results showed that FireFlyAODV has better performance in the terms of criteria of packet delivery ratio, throughput, number of lost packets, and end to end delay.

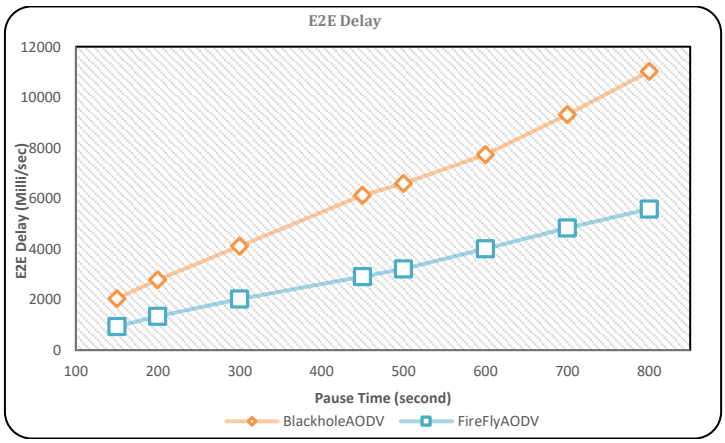

Fig. 5 end-to-end delay against time (seconds)

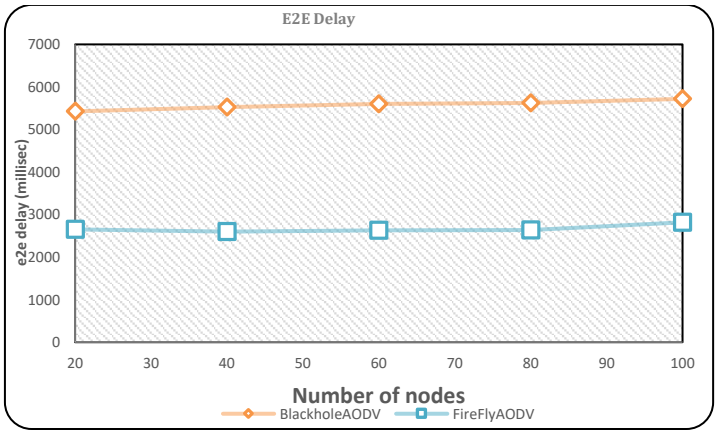

Fig. 6 end-to-end delay against nodes

Figure 5 and 6 show that the end-to-end delay for FIREFLYAODV compared to AODV under attack is significantly lower. This figure shows that the proposed method, FIREFLYAODV has better performance both at different times and in front of nodes and this argument indicates better performance of proposed model. Because the proposed method by detecting and preventing black

hole attacks does not allow this attack to send additional and destructive packets and does not waste processor time so packets arrive earlier to the destination.

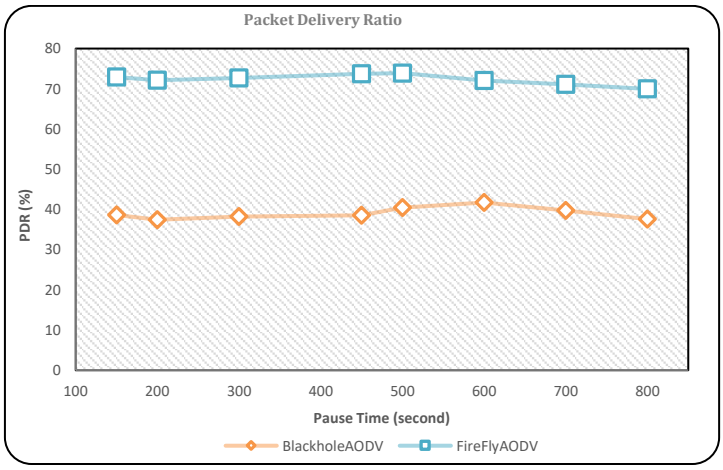

Fig. 7 packet delivery ratio against time (seconds)

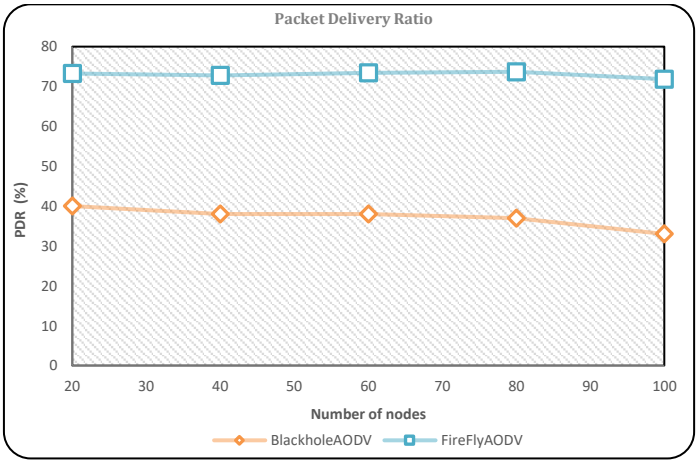

Fig. 8 packet delivery ratio against nodes

Figures 7 and 8 show the simulation we performed on the proposed method of twenty nodes at different times of 200, 400, 600, 800 and 1000. The results of simulation show that the proposed method FIREFLYAODV has better performance compared to AODV protocol under black hole attack at different times in terms ratio packet delivery and this argument demonstrated better performance of proposed model. Because it immediately detects the black hole attack and prevents the onset of this attack. The black hole attack resulted in a large number of remove packets but in the proposed method FIREFLYAODV by detecting and preventing this attack more packets arrive to the destination.

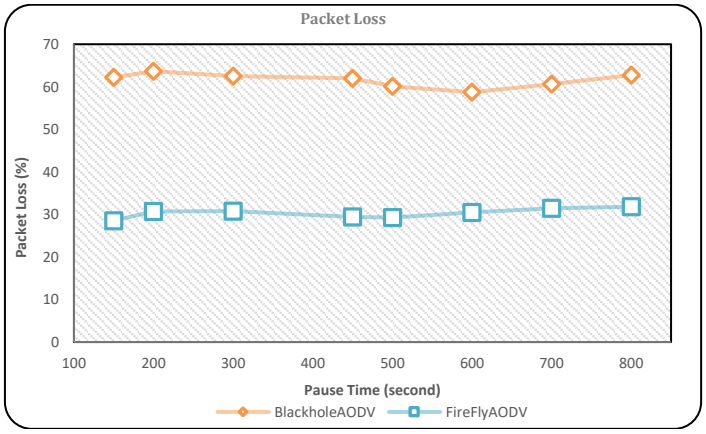

Fig. 9 The rate of lost packets against time (seconds)

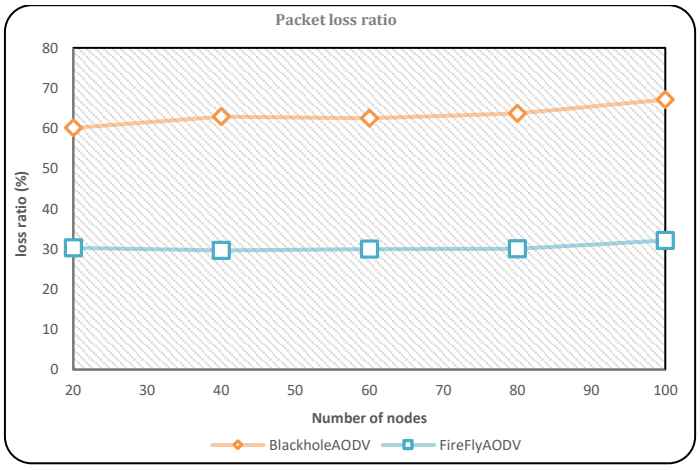

Fig. 10 The rate of lost packets against nodes

Figure 9 and 10 show that in proposed method FIREFLYAODV compared to AODV protocol under black hole attack at different times the number of lost packets has declined. The reason of lost packets ratio being lower is that the proposed method FireFlyAODV detects black hole attack early and prevents the onset of this attack. Consequently, it has a better impact on the effectiveness of the proposed algorithm FIREFLYAODV.

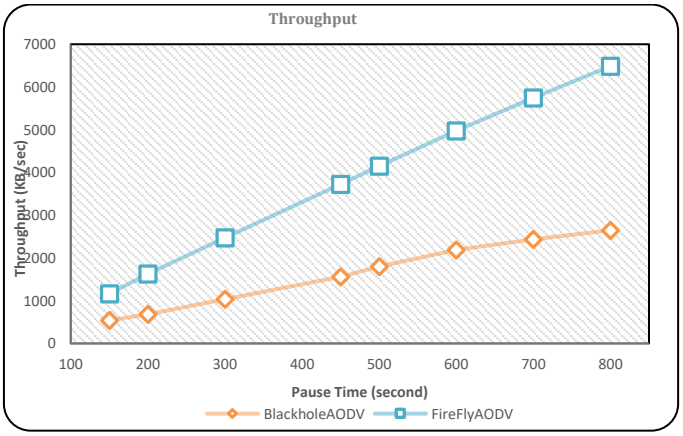

Fig. 11 Throughput against time (seconds)

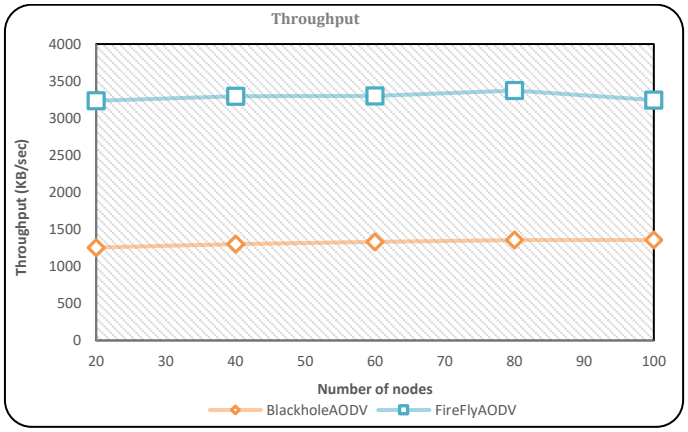

Fig. 12 Rate of lost packets against nodes

Figure 11 and 12 show that the proposed method FIREFLYAODV has better performance compared to AODV protocol under black hole attack at different times. The reason for this is that the proposed method makes more packets reach to the destination per time unit, therefore, FIREFLYAODV method has higher throughput on the same time unit compared to AODV protocol under attack.

7 Conclusion

In this article, we discussed the problem of secure routing on mobile ad hoc networks and studied the black hole attack which is one of the most important attacks that affect ad hoc networks. In this attack, the attacker node after drawing the packets of a node to his side, selectively throws away a group of them and sends the rest. This paper presents a simple scheme to detect black holes nodes on MANET. In the proposed algorithm, FireFlyAODV, we used the firefly algorithm to detect this attack. Firefly algorithm is a biologically motivated algorithm for multi-faceted optimizing applications that recently have been developed and used in many applications and for this, the factors of attractiveness of the algorithms and the objective function have been used. Then, to demonstrate the effectiveness of the proposed method (FireFlyAODV), we evaluated and compared this method with AODV protocol under black hole attack using the NS-2 simulator, and to demonstrate the performance of our method, we used the criteria of the number of lost packets, packets delivery ratio, end-to-end delay and throughput. The proposed method is more efficient compared to AODV protocol under black hole attack [8].

References

1. Deng, H., Li, W., Dharma, P. A., (2002). Routing security in wireless ad hoc networks. Communications Magazine, IEEE 40.10. 70-75
2. Seung-joon, L., Han, B., Shin, M., (2002). Robust routing in wireless ad hoc networks. Parallel Processing Workshops. International Conference on IEEE.
3. Patel, A., (2013). Stable Multicast Trees based on Ant Colony Optimization for Vehicular Ad Hoc Networks. IEEE.
4. Tamilarasan, S., (2012). Securing AODV Routing Protocol from Black Hole Attack. International Journal of Computer Science and Telecommunications, 3, 52-56.

5. Karlof, C., Wagner, D., (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1, 293-315.
6. Saetang, W., Charoenpanyasak, S., (2012). CAODV Free Blackhole Attack in Ad Hoc Networks. International Conference on Computer Networks and Communication Systems, 35, 63-68.
7. Yu Yao Lei, G., Xingwei, W., Cuixiang, L., (2010). Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. International Conference on Computer Networks and Communication Systems, 35, 54-60.
8. Dokurer, S., (2006). Simulation of Black hole attack in wireless Ad-hoc networks. Atilim University,10, 30-38